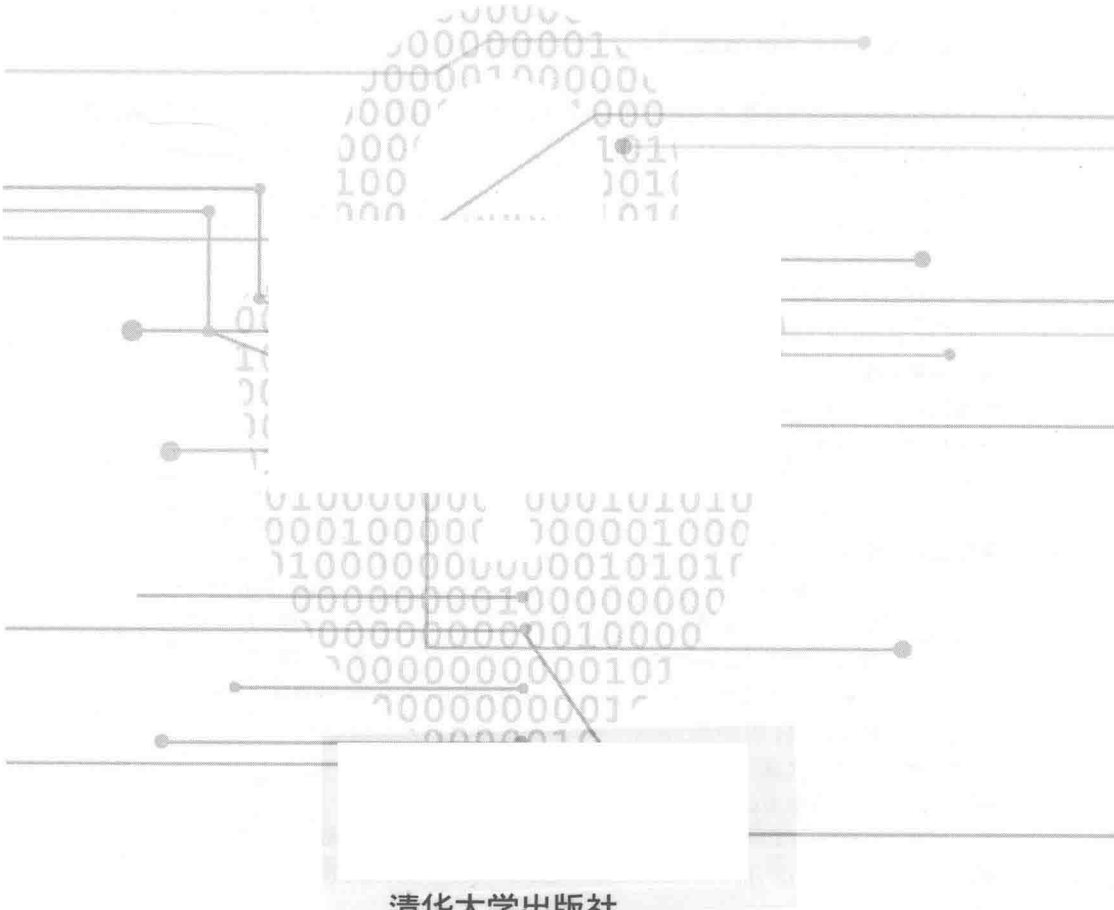
美国关键基础设施安全防护体系与策略

孙利民　吕世超　李红　文辉　编著

清华大学出版社

美国关键基础设施安全防护体系与策略

孙利民　吕世超　李红　文辉　编著



清华大学出版社

内 容 简 介

关键基础设施作为国家经济、社会运行的神经中枢，一旦遭到物理或网络攻击，将会严重危害国家安全和国计民生。因此，许多国家都已经将关键基础设施安全作为一个国家安全战略问题来对待。本书介绍了美国在关键基础设施安全防护领域的布局，归纳了相关研究项目的技术报告，提炼出了关键技术，总结了先进经验。这些技术和经验，对于我国开展关键基础设施安全防护工作具有重要参考价值。

本书可供高等院校信息安全相关专业的学生、教师，各级政府部门的决策者及企业技术主管等阅读参考。

图书在版编目(CIP)数据

美国关键基础设施安全防护体系与策略/孙利民等编著. —北京：清华大学出版社，2017
ISBN 978-7-302-48639-8

Ⅰ. ①美…　Ⅱ. ①孙…　Ⅲ. ①基础设施－安全防护－研究－美国　Ⅳ. ①F299.712

中国版本图书馆 CIP 数据核字(2017)第 261701 号

责任编辑：薛　慧
封面设计：何凤霞
责任校对：赵丽敏
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市铭诚印务有限公司
经　　销：全国新华书店
开　　本：170mm×230mm　　**印　　张**：18.75　　**字　　数**：346千字
版　　次：2017 年 12 月第 1 版　　**印　　次**：2017 年 12 月第1次印刷
定　　价：98.00 元

产品编号：074100-01

前　言

关键基础设施作为国家经济、社会运行的神经中枢，包括公共通信和信息服务、能源、交通、金融、关键制造、食品和农业、政府设施和服务、公共卫生等重要行业和领域的信息和物理设施。这些关键基础设施设备或系统一旦遭到物理或网络攻击，将会严重危害国家安全和国计民生。因此，许多国家都已经将关键基础设施安全作为国家安全战略问题。

随着近年来工业化和信息化的不断融合，越来越多的基础设施系统不再封闭，逐渐开放接入到公共网络中，这将给关键基础设施系统带来越发严峻的网络安全威胁。近年来发生的诸如 Stuxnet、Duqu、Flame、Havex、BlackEnergy 和乌克兰大规模断电等重大安全事件证明了关键基础设施容易受到网络攻击的严重危害，在一定程度上促进了世界各国对关键基础设施安全防护的高度重视。

美国为了应对日益严峻的关键基础设施网络攻击安全威胁，历届政府通过发布一系列政策文件或部署关键技术研究项目等方式，推动该领域的理论研究与技术研发工作。作者在研究美国关键基础设施安全防护进展中，深入调研了美国国土安全部、能源部、国家标准与技术研究院、国家科学基金会和国防部先进研究项目局等部门的相关工作，从国家政策、研发项目、安全实践等方面总结归纳了这些部门近年来的科研工作。希望以此为我国在该领域的科学研究与项目部署提供一些参考意见。由于国家体制、文化及体系结构上的差异，我们需要辩证地来分析美国在关键基础设施安全方面所做的工作，有借鉴性地探索适合我国国情的发展战略和具体实施方法。

本书由中国科学院信息工程研究所物联网信息安全技术北京市重点实验室组织撰写，多位作者合作完成。其中，孙利民负责全书的组稿，并主持各个章节的撰写，负责全书的审校。第 1 章由孙利民执笔完成，第 2、4、6 章由吕世超执笔完成，第 3 章、附录 A 和附录 B.1 由李红执笔完成，第 5 章、附录 B.2 和附录 B.3 由文辉执笔完成。

由于时间仓促及水平有限，本书难免有错漏之处，希望读者不吝批评指正。如有机会，我们将在后续的版本中更新修改，也会结合今后的研究工作继续补充内容。若有任何意见，请发送至 lvshichao_iie@126.com。

本书涉及的研究课题得到科技部国家重点研发计划项目“脆弱性分析与威胁态势感知技术”（项目编号：2016YFB0800202）、北京市科学技术委员会项目“国家关键基础设施安全监管平台核心技术研究”（项目编号：Z161100002616032）、国家自然科学基金项目“网络空间中工控设备快速发现与精细识别关键技术研究”（项目编号：U1536107）、国家自然科学基金项目“针对电网工控系统的协同入侵检测技术研究”（项目编号：61702506）等资助。

本书在撰写过程中得到了中国科学院信息工程研究所孟丹所长、孙德刚副所长等领导的指导和帮助，在此一并向他们表示衷心的感谢。

作者

2017 年 7 月于北京

目　录

图 目 录

第 1 章　关键基础设施安全概述

1.1　关键基础设施含义

关键基础设施是指公共通信和信息服务、能源、交通、水利、金融、化学、关键制造、食品和农业、政府设施和服务、公共卫生、国防军工、电子政务等重要行业和领域的重要信息和物理设施。作为经济、社会运行的神经中枢，这些设施一旦遭受来自物理和网络空间的破坏、丧失功能或者数据泄露，就可能严重危害国计民生、公共利益和国家安全。

1.1.1　中国政府高度重视关键信息基础设施安全

党的十八届三中全会通过了《关于全面深化改革若干重大问题的决定》(简称《决定》)[1]。《决定》明确指出，“加大依法管理网络力度，加快完善互联网管理领导体制，确保国家网络和信息安全。设立国家安全委员会，完善国家安全体制和国家安全战略，确保国家安全。”为了贯彻落实十八届三中全会精神，健全公共安全体系，领导中国从网络大国迈向网络强国，中央网络安全和信息化领导小组于 2014 年 2 月 27 日宣告成立。中共中央总书记、国家主席、中央军委主席习近平担任组长，国务院总理李克强和中央书记处书记刘云山担任副组长。自中央网络安全和信息化领导小组成立以来，中国领导人高度重视关键信息基础设施网络安全问题，在小组全体会议、座谈会等重要场合发表了一系列重要讲话，分析了如何正确处理网络安全和发展的关系，阐述了网络强国战略及其实施举措。

1. 中央网络安全和信息化领导小组第一次会议[2]

习近平总书记在 2014 年 2 月 27 日，主持召开了中央网络安全和信息化领导小组第一次全体会议，并发表了重要讲话。讲话指出：“没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济。”习总书记本次讲话提到的信息基础设施，主要

指在政治、经济、文化、社会、军事等领域用于信息采集、处理、传播和利用的信息系统和网络。

2. 习近平总书记4·19讲话[3]

习总书记在2016年4月19日网络安全和信息化座谈会上讲话指出,“加快构建关键信息基础设施安全保障体系。金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢,是网络安全的重中之重,也是可能遭到重点攻击的目标。‘物理隔离’防线可被跨网入侵,电力调配指令可被恶意篡改,金融交易信息可被窃取,这些都是重大风险隐患。不出问题则已,一出就可能导致交通中断、金融紊乱、电力瘫痪等问题,具有很大的破坏性和杀伤力。我们必须深入研究,采取有效措施,切实做好国家关键信息基础设施安全防护。”

3. 习近平主持召开国家安全工作座谈会[4]

习总书记在2017年2月17日召开的国家安全座谈会上强调,“要准确把握国家安全形势,牢固树立和认真贯彻总体国家安全观,以人民安全为宗旨,走中国特色国家安全道路,努力开创国家安全工作新局面,为中华民族伟大复兴中国梦提供坚实安全保障。”在部署对当前和今后一个时期国家安全工作时,明确提出,“要筑牢网络安全防线,提高网络安全保障水平,强化关键信息基础设施防护,加大核心技术研发力度和市场化引导,加强网络安全预警监测,确保大数据安全,实现全天候全方位感知和有效防护。”习总书记将关键信息基础设施安全问题作为国家安全问题来看待。由此可见,国家领导人高度重视关键信息基础设施安全。

4. 2016年3月政府工作报告[5]

李克强总理2016年3月5日在第十二届全国人民代表大会第四次会议上做的政府工作报告中多次提到了基础设施建设工作。在“十三五”时期主要目标任务和重大举措的推进新型城镇化和农业现代化,促进城乡区域协调发展方面指出:“加强重大基础设施建设,高铁营业里程达到3万公里、覆盖80%以上的大城市,新建改建高速公路通车里程约3万公里,实现城乡宽带网络全覆盖。”在2016年重点工作中的改善农村公共服务方面指出:“加大农村基础设施建设力度,新建改建农村公路20万公里,具备条件的乡镇和建制村要加快通硬化路、通客车。抓紧新一轮农村电网改造升级,两年内实现农村稳定可靠供电服务和平原地区机井通电全覆盖。实施饮水安全巩固提升工程。推动电子商务进农村。

建设美丽宜居乡村”。在安全生产和公共安全方面指出：“加强安全基础设施和防灾减灾能力建设，健全监测预警应急机制，提高气象服务水平，做好地震、测绘、地质等工作。完善和落实安全生产责任、管理制度和考核机制，实行党政同责、一岗双责、失职追责，严格监管执法，坚决遏制重特大安全事故发生，切实保障人民生命财产安全。”

分析政府工作报告中与基础设施相关的内容可知，基础设施的范围比信息基础设施要大，基础设施不仅包括用来保障金融、能源、电力、交通等领域系统正常运作的电信和广播电视等网络空间的系统和网络，还包括为人民生产生活提供公共服务的工程设施，如公路、铁路、电网、水利等物理空间设施。即基础设施既包括网络空间的信息基础设施，也包括物理空间的工程设施。

5. “一带一路”推进能源基础设施互联互通[6]

李克强总理在 2016 年 11 月 17 日主持召开的国家能源委员会会议上指出，“能源战略是国家发展战略的重要支柱，保障国家能源安全需要统筹国内国际两个大局，既要立足国内，又要深化国际合作，形成多元稳定的供给格局。要巩固与传统资源国家的互利合作，优化能源贸易结构，抓住‘一带一路’建设重大机遇，推进能源基础设施互联互通，加大国际产能合作，带动有竞争优势的能源装备出口。积极参与全球能源治理，推动国际能源秩序和治理体系朝着更加公正合理的方向发展。”

能源指煤炭、石油、天然气、生物质能和电力、热力以及其他直接或者通过加工、转换而取得有用能的各种资源[7]。作为基础设施的一个重要领域，能源是国民经济发展的重要物质基础。中国政府高度重视能源基础设施互联互通建设工作。

1.1.2　中国政府相关文件

1. 国务院

国务院办公厅于 2007 年 9 月 18 日发布了《关于开展重大基础设施安全隐患排查工作的通知》(国办发〔2007〕58 号)[8]，通知要求，重点做好“公路交通设施、铁路交通设施、水运交通设施、民航交通设施、大型水利设施、大型煤矿、重要电力设施、石油天然气设施、城市基础设施”九个对象的安全隐患排查工作。国务院办公厅指出的上述九类基础设施都属于重大、关键基础设施范畴，都是指那些关乎国计民生的核心基础设施。

国务院办公厅于2012年6月28日发布了文件《关于大力推进信息化发展和切实保障信息安全的若干意见》(国发〔2012〕23号)[9]。该文件在健全安全防护和管理,保障重点领域信息安全的保障工业控制系统安全方面指出:"加强核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要领域工业控制系统,以及物联网应用、数字城市建设中的安全防护和管理,定期开展安全检查和风险评估。重点对可能危及生命和公共财产安全的工业控制系统加强监管。对重点领域使用的关键产品开展安全测评,实行安全风险和漏洞通报制度。"工业控制系统广泛应用于上述领域的基础设施中,实现设施和系统的自动化控制和运行操作,是基础设施的核心组成部分。这些基础设施的安全防护重点就是保障工业控制系统的网络和物理安全。

国务院于2013年9月6日发布了文件《关于加强城市基础设施建设的意见》(国发〔2013〕36号)[10]。文件指出,城市基础设施是城市正常运行和健康发展的物质基础,并建议,"加强城市道路交通基础设施建设,加大城市管网建设和改造力度,加快污水和垃圾处理设施建设,加强生态园林建设。"城市基础设施是国家关键基础设施的缩影和典型代表,城市中的道路、水/电/天然气管网、污水和垃圾处理系统等组成了城市的骨架,这些基础设施的完善程度影响着城市的承载能力及人民的生活质量。

2. 工业和信息化部

工信部于2014年8月29日发布了《关于加强电信和互联网行业网络安全工作的指导意见》(工信部保〔2014〕368号)[11],在加强新技术新业务网络安全管理重点工作中指出:"加强对云计算、大数据、物联网、移动互联网、下一代互联网等新技术新业务网络安全问题的跟踪研究,对涉及提供公共电信和互联网服务的基础设施和业务系统要纳入通信网络安全防护管理体系,加快推进相关网络安全防护标准研制,完善和落实相应的网络安全防护措施。"提供公共电信和互联网服务的网络和系统都属于信息基础设施的范畴。

工信部于2011年10月27日发布了《关于加强工业控制系统信息安全管理的通知》(工信部协〔2011〕451号)[12]。通知指出:"数据采集与监控(SCADA)、分布式控制系统(DCS)、过程控制系统(PCS)、可编程逻辑控制器(PLC)等工业控制系统广泛运用于工业、能源、交通、水利以及市政等领域,用于控制生产设备的运行。一旦工业控制系统信息安全出现漏洞,将对工业生产运行和国家经济安全造成重大隐患。加强工业控制系统信息安全管理的重点领域包括核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、

城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。”上述关键基础设施都是指事关国家、经济发展命脉的重要工业控制设备、网络和系统。

3. 网络安全法

2016 年 11 月 7 日，第十二届全国人民代表大会常务委员会第二十四次会议通过了《中华人民共和国网络安全法》（简称《网络安全法》）[13]。该法案专门设立了一节对关键信息基础设施的运行安全做出了具体的法律规定，对关键信息基础设施运行安全不仅给出了定义，规定了如何实施安全保护，而且还从国家相关部门、行业、关键基础设施/网络运营者等不同层面分别规定了国家网信部门、行业主管单位、运营单位或企业等各自的义务与责任。

其中，《网络安全法》的第三章网络运行安全的第二节关键信息基础设施的运行安全的第三十一条规定：“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。”与其他定义相比，《网络安全法》对关键信息基础设施的定义又新增加了网络安全等级保护和重点保护的要求。

4. 国家互联网信息办公室

经中央网络安全和信息化领导小组批准，国家互联网信息办公室于 2016 年 12 月 27 日发布了《国家网络空间安全战略》（简称《战略》）[14]，将保护关键信息基础设施作为一项重点战略任务。《战略》指出：“国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏。坚持技术和管理并重、保护和震慑并举，着眼识别、防护、检测、预警、响应、处置等环节，建立实施关键信息基础设施保护制度，从管理、技术、人才、资金等方面加大投入，依法综合施策，切实加强关键信息基础设施安全防护。”《战略》不仅给出了关键信息基础设施较为全面的定义，还重点强调了信息基础设施和其关键数据的同等重要性。